PUBLICATION

Cyber Attack Information Sharing Will Bring Liability Protections to Companies

Authors: Alisa L. Chestler
December 23, 2015

On December 18, 2015, President Obama signed the 2016 Consolidated Appropriations Act. Included in this must-pass federal funding legislation is the Cybersecurity Act of 2015, which represents the most significant federal legislation to date addressing cybersecurity and cyber threats.

Cybersecurity Information Sharing Act

The most significant portion of the Cybersecurity Act comes in Title I, the "Cybersecurity Information Sharing Act" (CISA). The overriding intention of the CISA is to encourage private entities to report – voluntarily – any hacks, suspected hacks or other cyber threat indicators that they experience on their information systems. Notably, the CISA makes the Department of Homeland Security (DHS) the go-to agency for reporting cyber threats, providing much-needed clarity as to where private entities should report their cybersecurity issues.

Having received notice through this voluntary reporting system, DHS is empowered to facilitate the timely sharing of threat information and defensive measures with the business community. The goal is to create a real-time notification procedure for the dissemination of existing and potential cyber threats, and to head them off before they reach additional targets.

As an inducement to encourage information sharing, CISA contains liability protections for private entities, both for monitoring their information systems and for sharing information concerning cyber threat indicators with DHS. As to monitoring, CISA bars liability to third parties for any cause of action arising out of a private entity's monitoring of its information systems "for cybersecurity purposes." The catch, however, is that information obtained during monitoring cannot be used for any non-cybersecurity purposes. Private companies, therefore, will need to develop strict compliance standards to ensure that any information they obtain through CISA is not used for any other purposes.

With respect to information shared with DHS, private entities will not be liable for such information sharing, but again, the operation of the liability bar requires that the entity share the information in accord with the standards, and use the specific method that DHS establishes for such information sharing. These standards will be forthcoming from DHS, and private entities will want to review them carefully with counsel to ensure that any communications with DHS qualify for liability protection.

Privacy Concerns

Controversially, CISA has limited privacy protections for personally identifiable information (PII). Before sharing information about a cyber-threat indicator, the sharing entity is only required to remove PII that it "knows at the time" of sharing is "not directly related to a cybersecurity threat." Moreover, DHS is permitted to provide the information it receives to state and federal law enforcement authorities.

While these provisions will ease the burden on entities that report cyber incidents to DHS, loose privacy protections could risk the entity's goodwill among its customers, who may regard sharing of their private information with law enforcement as a significant breach of trust. While the CISA liability limitation as to third

parties mitigates legal concerns, business risk could still remain. Accordingly, entities would be wise to consult with counsel to determine the appropriate scope of any disclosure to DHS and to formulate an internal protocol for information sharing.

Special Considerations for the Health Care Industry

As it maintains particularly sensitive information on nearly every American citizen, preventing and responding to data breaches is of special concern to the health care industry. Accordingly, Title II of the Cybersecurity Act contains dedicated provisions for improving cybersecurity for health care providers.

Title II directs the Department of Health and Human Services (HHS), along with DHS, to convene a task force of health care industry stakeholders to analyze the particular cybersecurity challenges facing the health care industry and to establish a plan for implementing the real-time sharing of actionable cyber threat indicators with the federal government and others in the health care industry. The Act provides approximately 15 months for the task force to deliver recommendations to the health care industry on improving preparedness for and response to cybersecurity attacks.

The Act also calls for HHS, DHS and other health care industry stakeholders to develop a common set of voluntary, consensus-based industry guidelines and best practices for reducing cybersecurity risks and the adoption and implementation of safeguards to address threats.

Mobile Technology

As mobile technology continues to develop and become a driving force in both the economy and society, the Act directs DHS to prepare an unclassified study on mobile device security, assessing threats and making recommendations for the federal government. While this study will provide a plan for adoption of its recommendations only for government agencies, non-governmental entities also will be wise to review its recommendations to determine any security best practices in this ever-evolving field.

Conclusion

Many of the details of the Cybersecurity Act will be forthcoming over the next 12-18 months, as agency rulemaking takes place and the directed task force recommendations are issued. Baker Donelson will continue to monitor these developments. For more information on how the Act or future rulemaking may affect your business or related matters, contact the authors of this alert or any members of the Firm's Privacy and Information Security Team.